بسمه تعالی

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای
سازمان فناوری اطلاعات ایران
معاونت امنیت فضای تولید و تبادل اطلاعات

رفع چندین آسیب‌پذیری مهم در تلفن‌های همراه سامسونگ

خبر آسیب‌پذیری

شناسه سند ..... Maher_13990626….

نوع سند ..... گزارش فنی

شماره نگارش ۰,۱

تاریخ نگارش ۱۳۹۹/۰۶/۲۶

طبقه‌بندی سند ..... **عادی**

تهران، میدان آرژانتین، ابتدای بلوار بیهقی، نبش خیابان شانزدهم، ساختمان شماره ۱، سازمان فناوری اطلاعات ایران

(۰۲۱) ۴۲۶۵۰۰۰۰ (۰۲۱) ۴۲۶۵۰۰۰۰ cert.ir

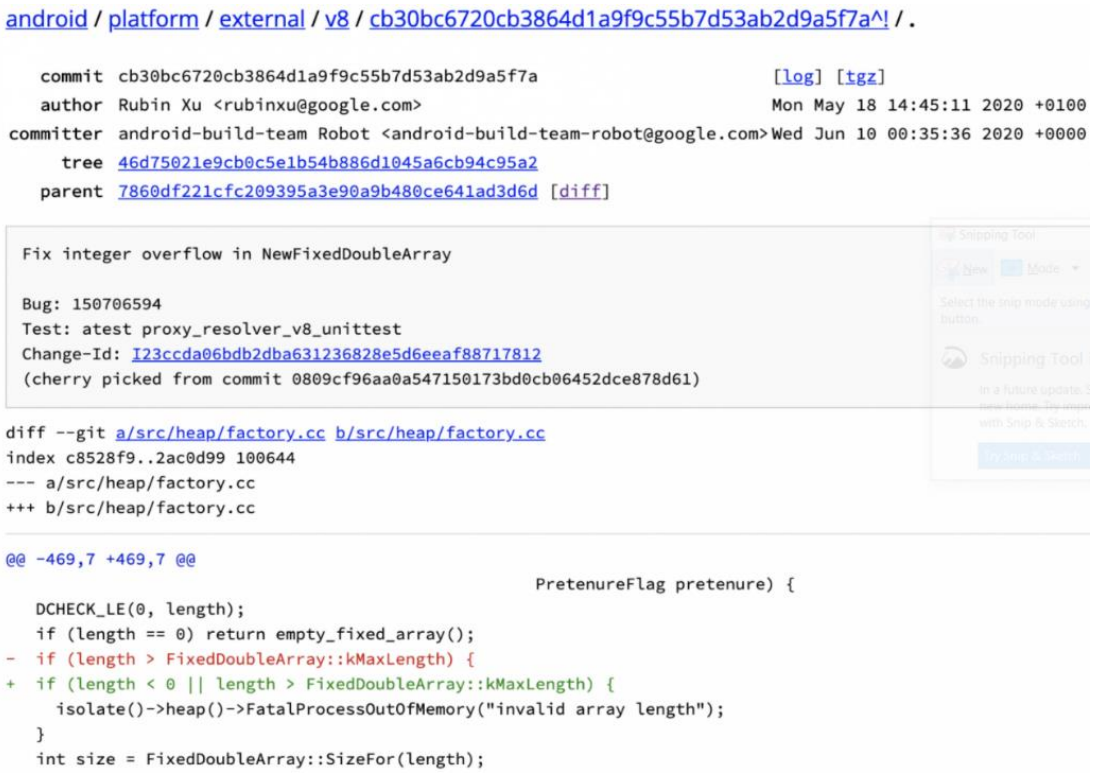
فهرست مطالب

۱ جزئیات آسیب‌پذیری و روش بهره‌برداری

اخیراً شرکت سامسونگ برای رفع برخی آسیب‌پذیری‌های بحرانی موجود در تلفن‌های همراه خود، بروزرسانی‌های امنیتی منتشر کرد. این بروزرسانی‌های امنیتی شامل تعداد زیادی وصله امنیتی می‌باشد که همه آسیب‌پذیری‌های مهم در بسیاری از نسخه‌های سیستم‌عامل Android را برطرف می‌کند. با این حال، بروزرسانی امنیتی منتشر شده در سپتامبر سال ۲۰۲۰، شامل تلفن همراه مدل Galaxy (SM-N960F) Note 9 نیز خواهد شد.

براساس گزارش‌های منتشر شده، اولین بروزرسانی، برای رفع آسیب‌پذیری موجود در گوشی سامسونگ 5G منتشر شد. این آسیب‌پذیری به گونه‌ای عمل می‌کند که بدون داشتن مجوز، می‌توان از دستوالعمل‌های USB debugging مرتبط با دستورات LTE و 5G استفاده کرد.

در میان آسیب‌پذیری‌های موجود در گوشی‌های سامسونگ، شدیدترین آسیب‌پذیری دارای شناسه "CVE-2020-0240"، Base Score 8.8 و شدت بحرانی می‌باشد که به واسطه نقص "integer overflow" موجود در سیستم‌عامل اندروید، منجر به اجرای کد از راه دور خواهد شد؛ به گفته محققان، این آسیب‌پذیری موجب می‌شود تا یک مهاجم از راه دور اختیارات کامل دستگاه شما را در بدست بگیرد. آسیب‌پذیری‌های دیگری نیز وجود دارد که این امکان را به مهاجم خواهند داد تا ارتباط کاربر را جهت کسب مجوز آنتن هوایی دور بزند و با قدرت بالاتری کد را مدیریت کند.



android / platform / external / v8 / cb30bc6720cb3864d1a9f9c55b7d53ab2d9a5f7a^! / .

```
commit cb30bc6720cb3864d1a9f9c55b7d53ab2d9a5f7a                    [log] [tgz]
author Rubin Xu <rubinxu@google.com>                               Mon May 18 14:45:11 2020 +0100
committer android-build-team Robot <android-build-team-robot@google.com> Wed Jun 10 00:35:36 2020 +0000
tree 46d75021e9cb0c5e1b54b886d1045a6cb94c95a2
parent 7860df221cfc209395a3e90a9b480ce641ad3d6d [diff]

Fix integer overflow in NewFixedDoubleArray

Bug: 150706594
Test: atest proxy_resolver_v8_unittest
Change-Id: I23ccda06bdb2dba631236828e5d6eeaf88717812
(cherry picked from commit 0809cf96aa0a547150173bd0cb06452dce878d61)

diff --git a/src/heap/factory.cc b/src/heap/factory.cc
index c8528f9..2ac0d99 100644
--- a/src/heap/factory.cc
+++ b/src/heap/factory.cc

@@ -469,7 +469,7 @@
                                                    PretenureFlag pretenure) {
   DCHECK_LE(0, length);
   if (length == 0) return empty_fixed_array();
-  if (length > FixedDoubleArray::kMaxLength) {
+  if (length < 0 || length > FixedDoubleArray::kMaxLength) {
     isolate()->heap()->FatalProcessOutOfMemory("invalid array length");
   }
   int size = FixedDoubleArray::SizeFor(length);
```

در صورت بهره‌برداری از آسیب‌پذیری با شدت بحرانی این اماکن فراهم خواهد شد که به یک برنامه مخرب اجازه داده شود تا به راحتی ارتباط کاربر را جهت بدست آوردن دسترسی‌های بیشتر دور بزند.

در جداول زیر، دیگر آسیب‌پذیرهایی که در بروزرسانی منتشر شده رفع شده‌اند را مشاهده می‌کنید.

- **Framework**

CVE	نوع حمله	شدت حمله	نسخه AOSP بروزرسانی شده
CVE-2020-0240	RCE	بالا	10
CVE-2020-0238	EoP	بالا	8.0, 8.1, 9, 10
CVE-2020-0257	EoP	بالا	10
CVE-2020-0239	ID	بالا	9, 10
CVE-2020-0249	ID	بالا	8.0, 8.1, 9, 10
CVE-2020-0258	ID	بالا	10
CVE-2020-0247	DoS	بالا	8.0, 8.1, 10

- **Media Framework**

CVE	نوع حمله	شدت حمله	نسخه AOSP بروزرسانی شده
CVE-2020-0241	EoP	بالا	8.0, 8.1, 9, 10
CVE-2020-0242	EoP	بالا	8.0, 8.1, 9, 10
CVE-2020-0243	EoP	بالا	8.0, 8.1, 9, 10

- **System**

CVE	نوع حمله	شدت حمله	نسخه AOSP بروزرسانی شده
CVE-2020-0108	EoP	بالا	8.1, 9, 10
CVE-2020-0256	EoP	بالا	8.0, 8.1, 9, 10
CVE-2020-0248	ID	بالا	10
CVE-2020-0250	ID	بالا	10

در خصوص گوشی‌های مدل Galaxy شرکت سامسونگ، انتشار بروزرسانی‌ها آغاز شده است و آخرین وصله امنیتی برای تاریخ ۰۱-۰۸-۲۰۲۰ ثبت شده است، که این مسئله نشان می‌دهد آسیب‌پذیرهایی که منجر به افزایش سطح دسترسی (EoP) می‌شوند و با بروزرسانی امنیتی منتشر شده در تاریخ ۰۵-۰۸-۲۰۲۰ وصله شده‌اند، هنوز هم قابل بهره‌برداری می‌باشند.

آسیب‌پذیری با شناسه "CVE-2020-0259" و Base Score 7.8 نیز می‌تواند یک مهاجم محلی را قادر سازد که با افزایش تمام امتیازات ، کد دلخواه خود را بر روی دستگاهی که وصله نشده است اجرا کند و منجر به افزایش سطح دسترسی خود شود.

۲ توصیه امنیتی

کارشناسان به کابرانی که از گوشی‌های سامسونگ استفاده می‌کنند توصیه کردند که هر چه سریع‌تر دستگاه‌های اندرویدی خود را بروزرسانی کنند تا از گزند این آسیب‌پذیری‌ها در امان باشند، همچنین کاربران باید از فعال بود گزینه "بروزرسانی خودکار" در گوشی خود، اطمینان حاصل کنند.

۳ منبع

[1] https://gbhackers.com/samsung-security-updates/